FIG.1

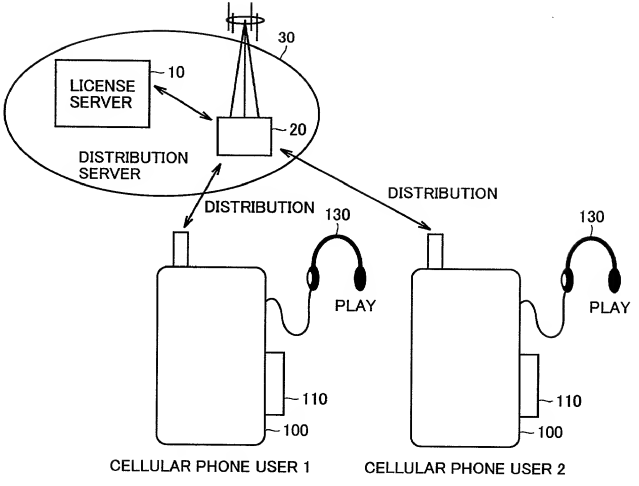

30
LICENSE SERVER
10
20
DISTRIBUTION SERVER
DISTRIBUTION
DISTRIBUTION
130
130
PLAY
PLAY
110
110
100
100
CELLULAR PHONE USER 1
CELLULAR PHONE USER 2

FIG.2A

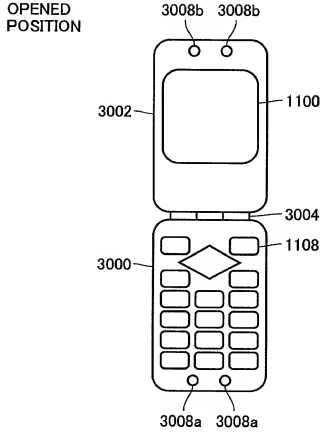


FIG.2B

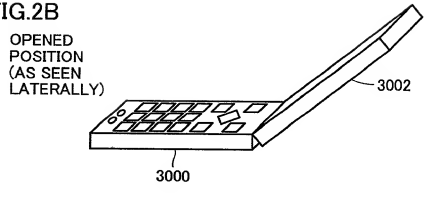


FIG.2C

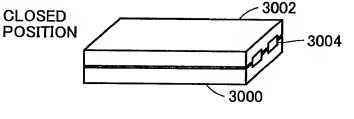


FIG.3

NAME	ATTRIBUTE	HELD/PRODUCED AT	FUNCTION & CHARACTERISTIC
Data	CONTENT DATA	DISTRIBUTION SERVER	E.G., MUSIC DATA
Kc	LICENSE KEY		KEY FOR DECRYPTING ENCRYPTED CONTENT DATA
[Data]Kc	ENCRYPTED CONTENT DATA		CONTENT DATA ENCRYPTED DECRYPTABLE WITH COMMON KEY Kc. DISTRIBUTED IN THIS FORM FROM DISTRIBUTION SERVER.
Data-inf	ADDITIONAL INFORMATION		E.G., COPYRIGHT OF CONTENT DATA OR PLAINTEXT INFORMATION RELATED TO SERVER ACCESS
CONTENT ID	INFORMATION ON CONTENT		CODE FOR IDENTIFYING CONTENT DATA Data
LICENSE ID	INFORMATION OF LICENSE		MANAGEMENT CODE CAPABLE OF SPECIFYING ISSUANCE OF LICENSE (ALSO CAPABLE OF IDENTIFYING IT INCLUDING CONTENT ID)
AC	LICENSE PURCHASING CONDITION		DESIGNATED BY USER (E.G., NO. OF LICENSES, LIMITATION ON FUNCTION)
AC1	ACCESS RESTRICTION INFORMATION		RESTRICTION ON MEMORY ACCESS (E.G., NO. OF TIMES OF REPRODUCTION ALLOWED)
AC2	REPRODUCTION CIRCUIT CONTROL INFORMATION		CONTROL INFORMATION IN CONTENT REPRODUCTION CIRCUIT (CELLULAR PHONE) (E.G., WHETHER REPRODUCTION IS ALLOWED/DISALLOWED)

FIG.4

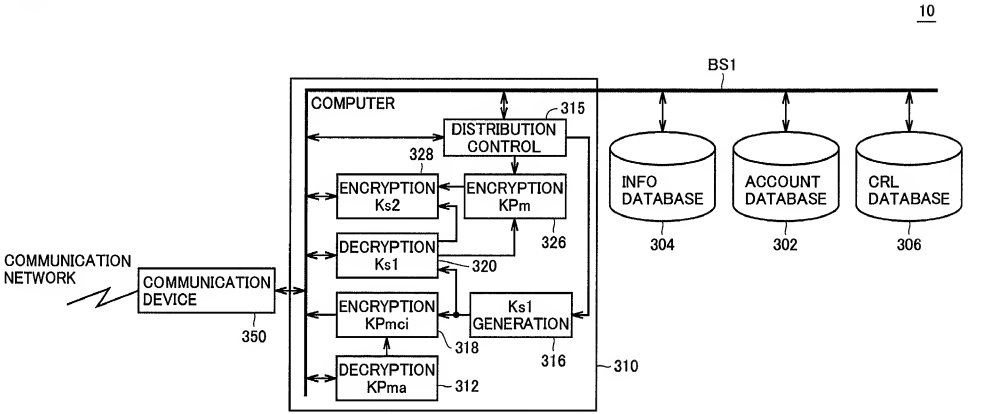
NAME	ATTRIBUTE	HELD/PRODUCED AT	FUNCTION & CHARACTERISTIC
CRL	INFORMATION OF CLASS REVOCATION LIST	DISTRIBUTION SERVER MEMORY CARD	DATA OF CLASSES ON CLASS REVOCATION LIST
CRL_dat		DISTRIBUTION SERVER	INFORMATION FOR UPDATING THE VERSION OF CLASS REVOCATION LIST (IN THE FORM OF DIFFERENTIAL DATA)
CRL_ver		MEMORY CARD	INFORMATION OF VERSION OF CLASS REVOCATION LIST
KPpn	PUBLIC ENCRYPTION KEY (ASYMMETRIC KEY)	CELLULAR PHONE	DECRYPTABLE WITH Kpn. RECORDED IN THE FORM OF {KPpn//Crtfn}KPma WHEN SHIPPED. ＊DIFFERENT FOR EACH CELLULAR PHONE TYPE n.
KPmci	PUBLIC ENCRYPTION KEY (ASYMMETRIC KEY)	MEMORY CARD	DECRYPTABLE WITH Kmci. RECORDED IN THE FORM OF {KPmci//Cmci}KPma WHEN SHIPPED. ＊DIFFERENT FOR EACH MEMORY CARD TYPE i.
Kpn	SECRET DECRYPTION KEY	CELLULAR PHONE	DECRYPTION KEY UNIQUE TO CONTENT REPRODUCTION CIRCUIT (CELLULAR PHONE). ＊DIFFERENT FOR EACH CELLULAR PHONE TYPE n.
Kmci	SECRET DECRYPTION KEY	MEMORY CARD	DECRYPTION KEY UNIQUE TO MEMORY CARD. ＊DIFFERENT FOR EACH MEMORY CARD TYPE i.
Crtfn	CLASS CERTIFICATE	CELLULAR PHONE	CONTENT REPRODUCTION CIRCUIT CLASS CERTIFICATE.HAS AUTHENTICATION FUNCTION. RECORDED IN THE FORM OF {KPpn//Crtfn}KPma WHEN SHIPPED. ＊DIFFERENT FOR EACH CELLULAR PHONE CLASS n.
Cmci		MEMORY CARD	MEMORY CARD CLASS CERTIFICATE.HAS AUTHENTICATION FUNCTION. RECORDED IN THE FORM OF {KPmci//Cmci}KPma WHEN SHIPPED. ＊DIFFERENT FOR EACH MEMORY CARD CLASS i.

FIG.5

NAME	ATTRIBUTE	HELD/PRODUCED AT	FUNCTION & CHARACTERISTIC
Ks1	COMMON KEY	DISTRIBUTION SERVER	GENERATED FOR EACH DISTRIBUTION SESSION
Ks2		MEMORY CARD	GENERATED FOR EACH DISTRIBUTION/REPRODUCTION SESSION
Ks3		CELLULAR PHONE	GENERATED FOR EACH REPRODUCTION SESSION
Km	SECRET DECRYPTION KEY	MEMORY CARD	DECRYPTION KEY UNIQUE TO EACH MEMORY CARD DATA ENCRYPTED WITH KPm IS DECRYPTABLE WITH Km.
KPm	PUBLIC ENCRYPTION KEY (ASYMMETRIC KEY)	MEMORY CARD	ENCRYPTION KEY UNIQUE TO EACH MEMORY CARD
KPma	PUBLIC AUTHENTICATION KEY	DISTRIBUTION SERVER	SHARED THROUGHOUT THE DISTRIBUTION SYSTEM.

TOO280 858T660

FIG.6



T00280 858T660

FIG.7

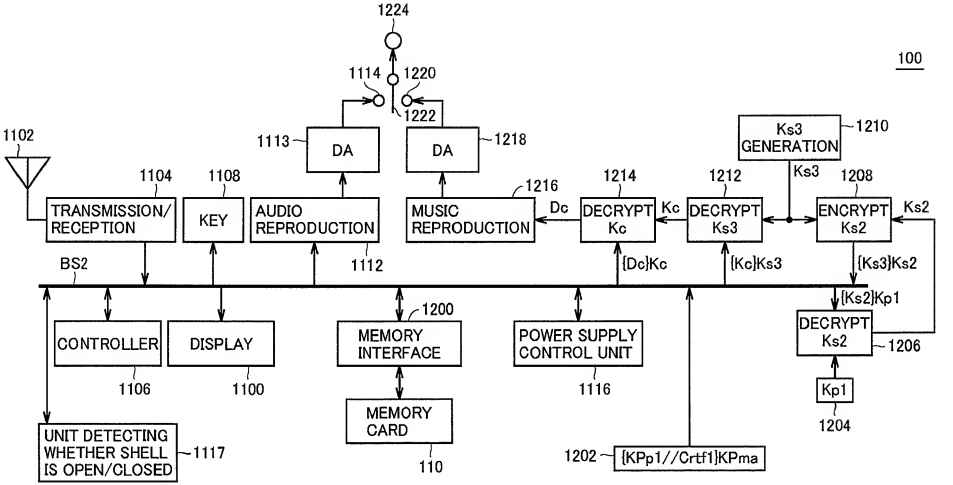


FIG.8

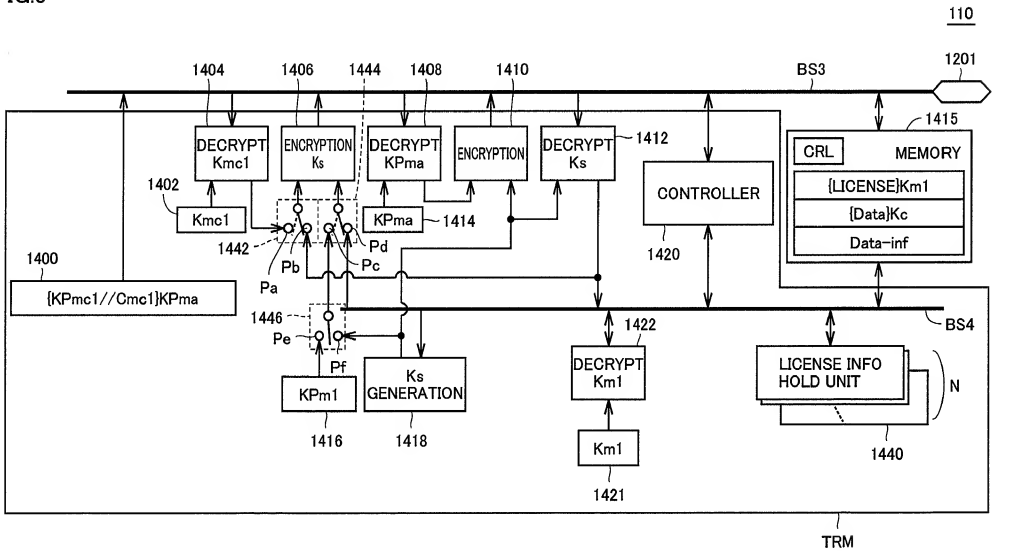

110
1404
1406
1444
1408
1410
BS3
1201
DECRYPT Kmc1
ENCRYPTION Ks
DECRYPT KPma
ENCRYPTION
DECRYPT Ks
1412
1415
CRL
MEMORY
{LICENSE}Km1
{Data}Kc
Data-inf
CONTROLLER
1420
1402
Kmc1
KPma
1414
1442
Pd
Pb
Pc
Pa
1400
{KPmc1//Cmc1}KPma
1446
Pe
Pf
BS4
1422
DECRYPT Km1
LICENSE INFO HOLD UNIT
N
KPm1
Ks GENERATION
1416
1418
Km1
1421
1440
TRM

FIG.9

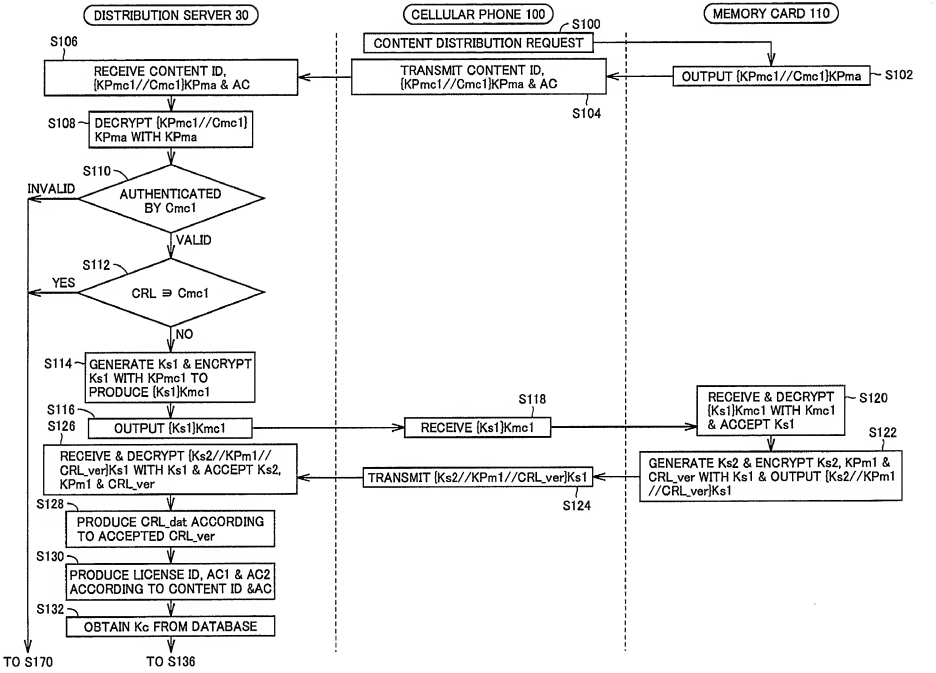

DISTRIBUTION SERVER 30
CELLULAR PHONE 100
MEMORY CARD 110
S100
CONTENT DISTRIBUTION REQUEST
S102
OUTPUT [KPmc1//Cmc1]KPma
S104
TRANSMIT CONTENT ID, [KPmc1//Cmc1]KPma & AC
S106
RECEIVE CONTENT ID, [KPmc1//Cmc1]KPma & AC
S108
DECRYPT [KPmc1//Cmc1] KPma WITH KPma
S110
AUTHENTICATED BY Cmc1
INVALID
VALID
S112
CRL ∋ Cmc1
YES
NO
S114
GENERATE Ks1 & ENCRYPT Ks1 WITH KPmc1 TO PRODUCE [Ks1]Kmc1
S116
S126
OUTPUT [Ks1]Kmc1
S118
RECEIVE [Ks1]Kmc1
S120
RECEIVE & DECRYPT [Ks1]Kmc1 WITH Kmc1 & ACCEPT Ks1
S122
GENERATE Ks2 & ENCRYPT Ks2, KPm1 & CRL_ver WITH Ks1 & OUTPUT [Ks2//KPm1 //CRL_ver]Ks1
S124
TRANSMIT [Ks2//KPm1//CRL_ver]Ks1
RECEIVE & DECRYPT [Ks2//KPm1// CRL_ver]Ks1 WITH Ks1 & ACCEPT Ks2, KPm1 & CRL_ver
S128
PRODUCE CRL_dat ACCORDING TO ACCEPTED CRL_ver
S130
PRODUCE LICENSE ID, AC1 & AC2 ACCORDING TO CONTENT ID &AC
S132
OBTAIN Kc FROM DATABASE
TO S170
TO S136

FIG.10

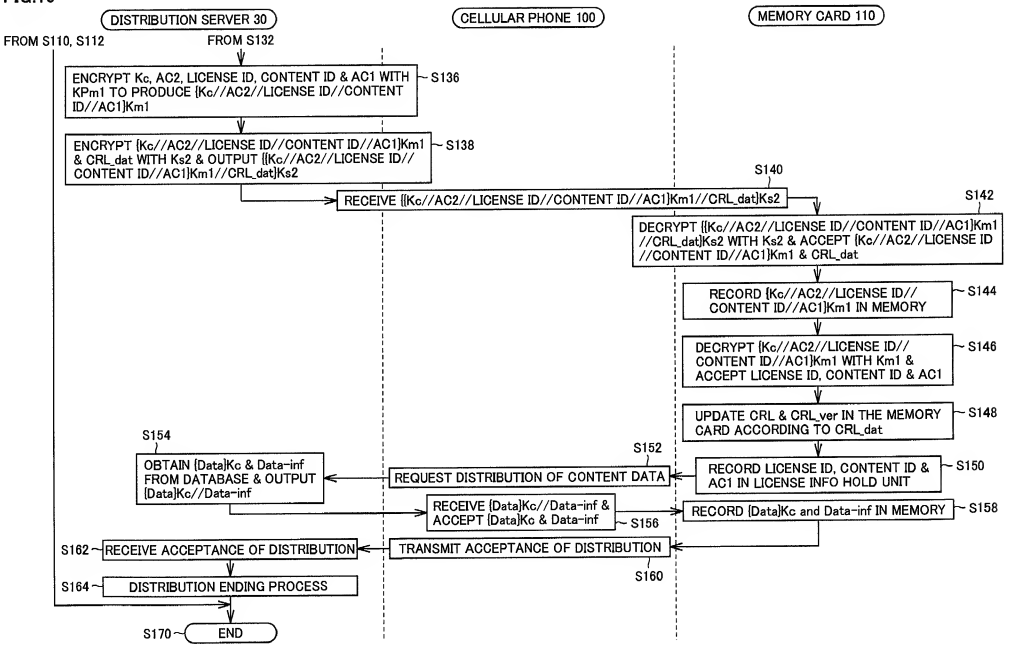

DISTRIBUTION SERVER 30
CELLULAR PHONE 100
MEMORY CARD 110
FROM S110, S112
FROM S132
ENCRYPT Kc, AC2, LICENSE ID, CONTENT ID & AC1 WITH KPm1 TO PRODUCE [Kc//AC2//LICENSE ID//CONTENT ID//AC1]Km1
S136
ENCRYPT [Kc//AC2//LICENSE ID//CONTENT ID//AC1]Km1 & CRL_dat WITH Ks2 & OUTPUT [[Kc//AC2//LICENSE ID//CONTENT ID//AC1]Km1//CRL_dat]Ks2
S138
S140
RECEIVE [[Kc//AC2//LICENSE ID//CONTENT ID//AC1]Km1//CRL_dat]Ks2
S142
DECRYPT [[Kc//AC2//LICENSE ID//CONTENT ID//AC1]Km1//CRL_dat]Ks2 WITH Ks2 & ACCEPT [Kc//AC2//LICENSE ID//CONTENT ID//AC1]Km1 & CRL_dat
RECORD [Kc//AC2//LICENSE ID//CONTENT ID//AC1]Km1 IN MEMORY
S144
DECRYPT [Kc//AC2//LICENSE ID//CONTENT ID//AC1]Km1 WITH Km1 & ACCEPT LICENSE ID, CONTENT ID & AC1
S146
UPDATE CRL & CRL_ver IN THE MEMORY CARD ACCORDING TO CRL_dat
S148
S154
OBTAIN [Data]Kc & Data-inf FROM DATABASE & OUTPUT [Data]Kc//Data-inf
S152
REQUEST DISTRIBUTION OF CONTENT DATA
RECORD LICENSE ID, CONTENT ID & AC1 IN LICENSE INFO HOLD UNIT
S150
RECEIVE [Data]Kc//Data-inf & ACCEPT [Data]Kc & Data-inf
S156
RECORD [Data]Kc and Data-inf IN MEMORY
S158
S162
RECEIVE ACCEPTANCE OF DISTRIBUTION
TRANSMIT ACCEPTANCE OF DISTRIBUTION
S160
S164
DISTRIBUTION ENDING PROCESS
S170
END

FIG.11

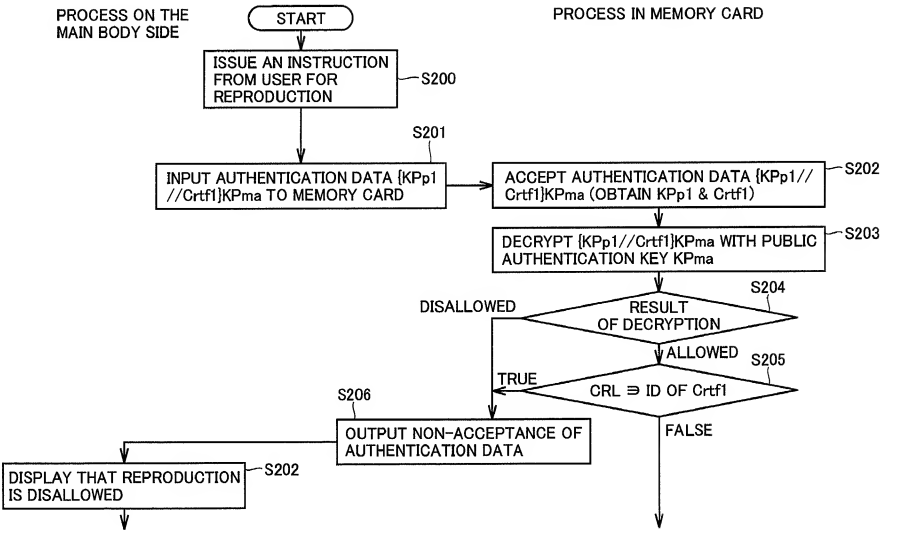

PROCESS ON THE MAIN BODY SIDE
START
ISSUE AN INSTRUCTION FROM USER FOR REPRODUCTION
S200
S201
INPUT AUTHENTICATION DATA {KPp1 //Crtf1}KPma TO MEMORY CARD
PROCESS IN MEMORY CARD
ACCEPT AUTHENTICATION DATA {KPp1// Crtf1}KPma (OBTAIN KPp1 & Crtf1)
S202
DECRYPT {KPp1//Crtf1}KPma WITH PUBLIC AUTHENTICATION KEY KPma
S203
S204
DISALLOWED
RESULT OF DECRYPTION
ALLOWED
S205
TRUE
CRL ∋ ID OF Crtf1
S206
FALSE
OUTPUT NON-ACCEPTANCE OF AUTHENTICATION DATA
DISPLAY THAT REPRODUCTION IS DISALLOWED
S202

FIG.12

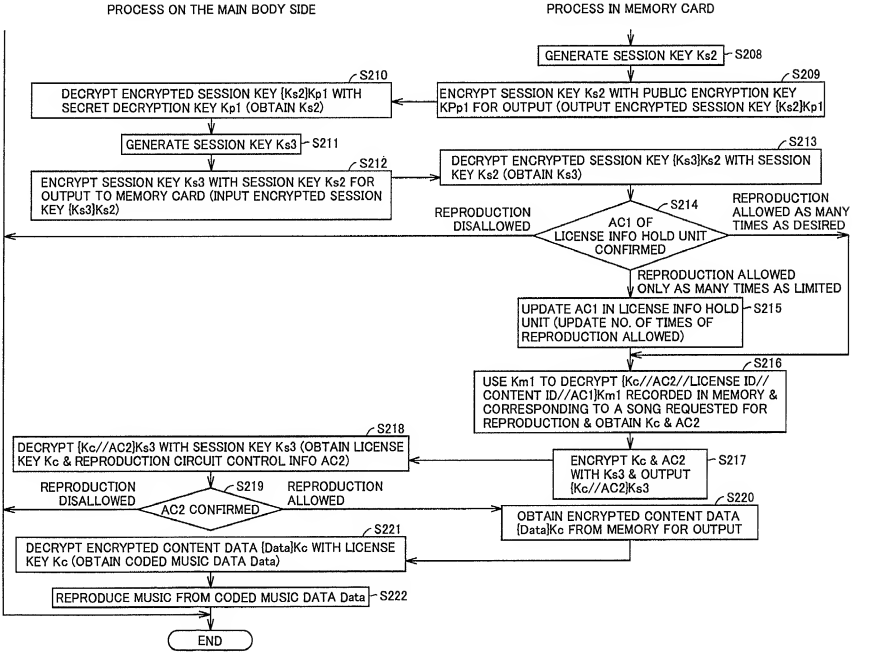

PROCESS ON THE MAIN BODY SIDE
PROCESS IN MEMORY CARD
GENERATE SESSION KEY Ks2
S208
S209
ENCRYPT SESSION KEY Ks2 WITH PUBLIC ENCRYPTION KEY KPp1 FOR OUTPUT (OUTPUT ENCRYPTED SESSION KEY {Ks2}Kp1
S210
DECRYPT ENCRYPTED SESSION KEY {Ks2}Kp1 WITH SECRET DECRYPTION KEY Kp1 (OBTAIN Ks2)
GENERATE SESSION KEY Ks3
S211
S213
DECRYPT ENCRYPTED SESSION KEY {Ks3}Ks2 WITH SESSION KEY Ks2 (OBTAIN Ks3)
S212
ENCRYPT SESSION KEY Ks3 WITH SESSION KEY Ks2 FOR OUTPUT TO MEMORY CARD (INPUT ENCRYPTED SESSION KEY {Ks3}Ks2)
S214
AC1 OF LICENSE INFO HOLD UNIT CONFIRMED
REPRODUCTION DISALLOWED
REPRODUCTION ALLOWED AS MANY TIMES AS DESIRED
REPRODUCTION ALLOWED ONLY AS MANY TIMES AS LIMITED
UPDATE AC1 IN LICENSE INFO HOLD UNIT (UPDATE NO. OF TIMES OF REPRODUCTION ALLOWED)
S215
S216
USE Km1 TO DECRYPT {Kc//AC2//LICENSE ID// CONTENT ID//AC1}Km1 RECORDED IN MEMORY & CORRESPONDING TO A SONG REQUESTED FOR REPRODUCTION & OBTAIN Kc & AC2
S218
DECRYPT {Kc//AC2}Ks3 WITH SESSION KEY Ks3 (OBTAIN LICENSE KEY Kc & REPRODUCTION CIRCUIT CONTROL INFO AC2)
ENCRYPT Kc & AC2 WITH Ks3 & OUTPUT {Kc//AC2}Ks3
S217
REPRODUCTION DISALLOWED
S219
AC2 CONFIRMED
REPRODUCTION ALLOWED
S220
OBTAIN ENCRYPTED CONTENT DATA {Data}Kc FROM MEMORY FOR OUTPUT
S221
DECRYPT ENCRYPTED CONTENT DATA {Data}Kc WITH LICENSE KEY Kc (OBTAIN CODED MUSIC DATA Data)
REPRODUCE MUSIC FROM CODED MUSIC DATA Data
S222
END

FIG.13

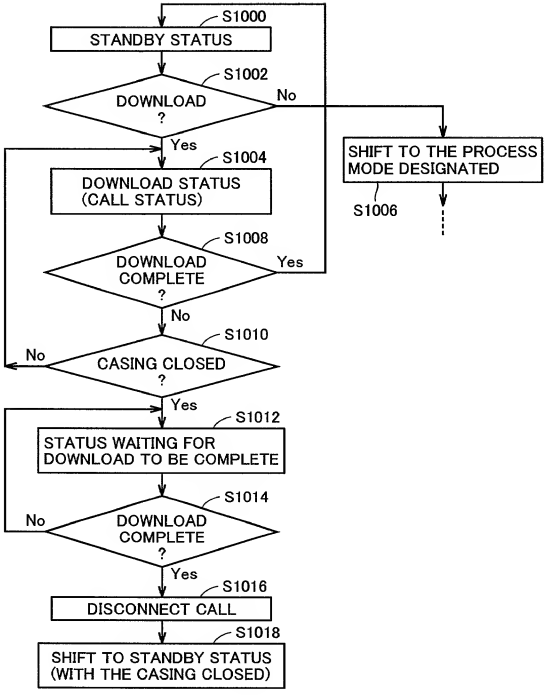

S1000
STANDBY STATUS
S1002
DOWNLOAD ?
No
Yes
SHIFT TO THE PROCESS MODE DESIGNATED
S1006
S1004
DOWNLOAD STATUS (CALL STATUS)
S1008
DOWNLOAD COMPLETE ?
Yes
No
S1010
CASING CLOSED ?
No
Yes
S1012
STATUS WAITING FOR DOWNLOAD TO BE COMPLETE
S1014
DOWNLOAD COMPLETE ?
No
Yes
S1016
DISCONNECT CALL
S1018
SHIFT TO STANDBY STATUS (WITH THE CASING CLOSED)

FIG.14

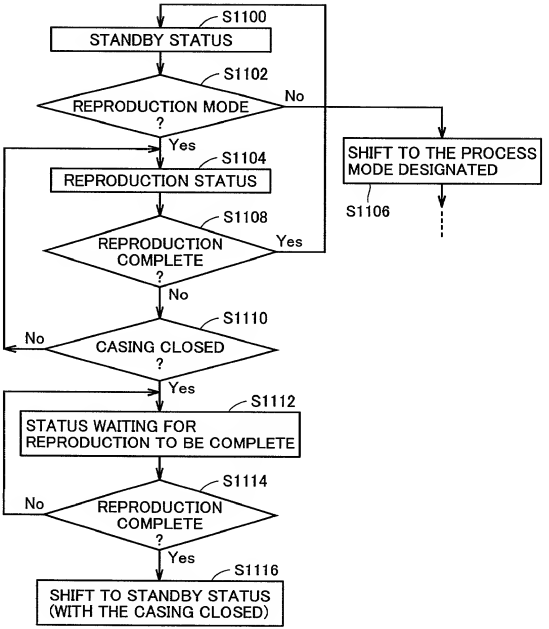

S1100
STANDBY STATUS
S1102
REPRODUCTION MODE ?
No
Yes
SHIFT TO THE PROCESS MODE DESIGNATED
S1106
S1104
REPRODUCTION STATUS
S1108
REPRODUCTION COMPLETE ?
Yes
No
S1110
CASING CLOSED ?
No
Yes
S1112
STATUS WAITING FOR REPRODUCTION TO BE COMPLETE
S1114
REPRODUCTION COMPLETE ?
No
Yes
S1116
SHIFT TO STANDBY STATUS (WITH THE CASING CLOSED)

FIG.15

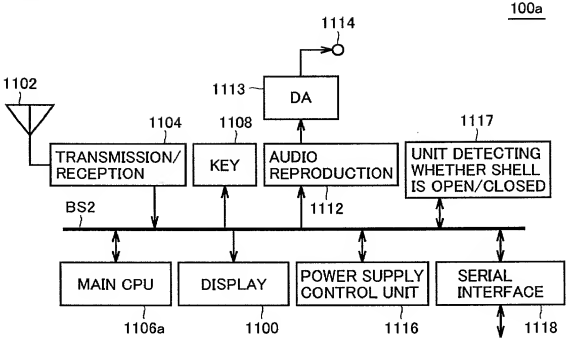
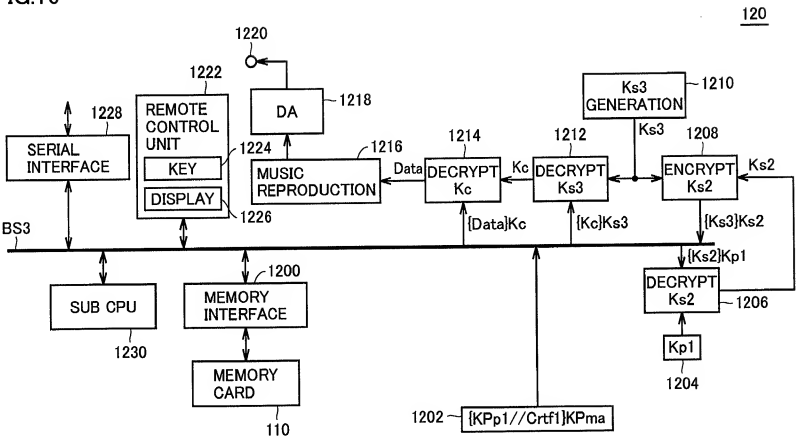

100a
1114
1102
1113
DA
1104
1108
1117
TRANSMISSION/
RECEPTION
KEY
AUDIO
REPRODUCTION
UNIT DETECTING
WHETHER SHELL
IS OPEN/CLOSED
BS2
1112
MAIN CPU
DISPLAY
POWER SUPPLY
CONTROL UNIT
SERIAL
INTERFACE
1106a
1100
1116
1118

FIG.16


120
1220
1222
REMOTE CONTROL UNIT
KEY
DISPLAY
1224
1226
DA
1218
1228
SERIAL INTERFACE
MUSIC REPRODUCTION
1216
Data
1214
DECRYPT Kc
Kc
1212
DECRYPT Ks3
Ks3 GENERATION
1210
Ks3
1208
ENCRYPT Ks2
Ks2
BS3
{Data}Kc
{Kc}Ks3
{Ks3}Ks2
{Ks2}Kp1
DECRYPT Ks2
1206
Kp1
1204
1200
MEMORY INTERFACE
SUB CPU
1230
MEMORY CARD
110
1202
{KPp1//Crtf1}KPma

T00280 "8587E660

FIG.17

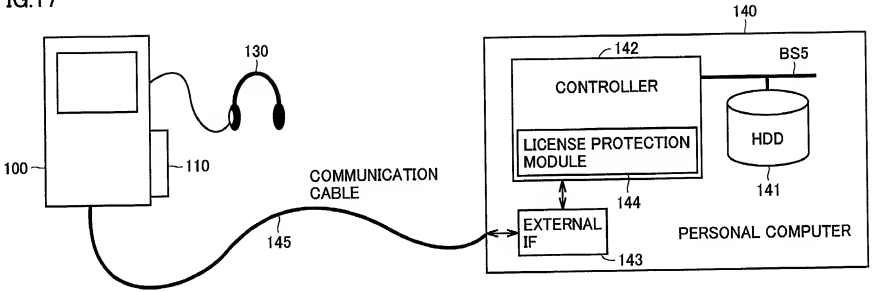
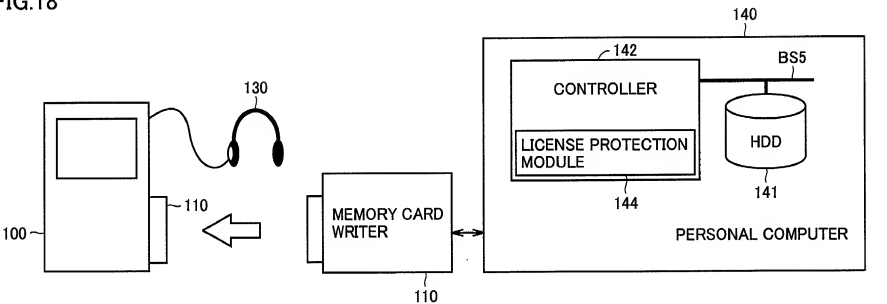


FIG.18


140
142
BS5
CONTROLLER
130
LICENSE PROTECTION MODULE
HDD
110
144
141
100
MEMORY CARD WRITER
PERSONAL COMPUTER
110

TOD280 8587660

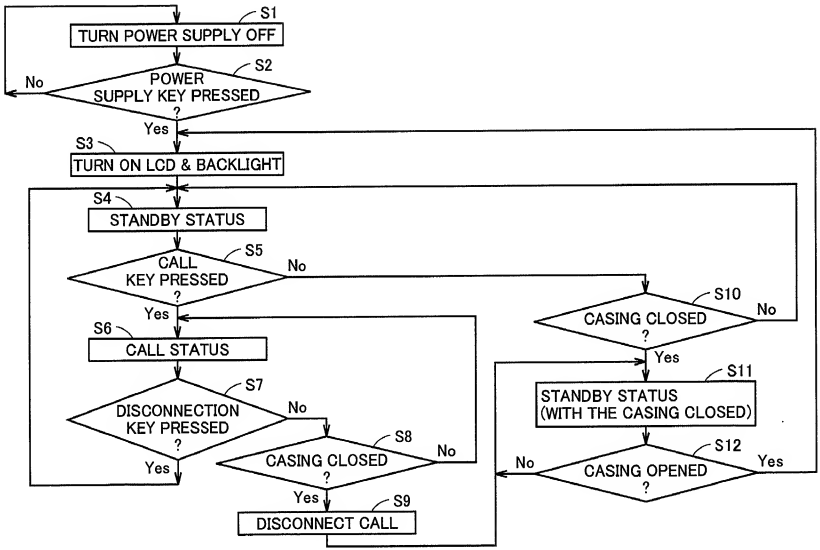



FIG.19 PRIOR ART